

## Plano de Ensino – II Quadrimestre 2024

[http://hostel.ufabc.edu.br/~edson.iwaki/?page\\_id=1298](http://hostel.ufabc.edu.br/~edson.iwaki/?page_id=1298)

Teoria Aritmética dos Números II -

Docente: Edson Ryoji Okamoto Iwaki – [edson.iwaki@ufabc.edu.br](mailto:edson.iwaki@ufabc.edu.br)

Horário: Segunda-feira: 19:00h – 21:00h – sala 305-2 – SA

quarta-feira: 21:00h-23:00h – sala 305-2 – SA

Ementa:

Congruências: solução de congruências, o Teorema Chinês dos Restos. Solução de congruências polinomiais. Redução de solução de congruência polinomial módulo potência de primo. Raízes primitivas e potências de resíduos.

Congruências de grau 2 módulo primo  $p$ . Resíduos quadráticos, reciprocidade quadrática, o símbolo de Jacobi, formas quadráticas binárias. Equivalência e redução de formas quadráticas binárias. Soma de dois quadrados. Formas quadráticas binárias positivamente definidas. Função maior inteiro. Funções aritméticas. Fórmula de inversão de Moebius. Funções recorrentes.

Cronograma (aproximado) de aulas:

Aula 1: Resolução de congruências quadráticas da forma  $ax^2+bx+c=0 \pmod{p}$ . Resíduos quadráticos de um primo ímpar  $p$ . Resíduos não quadráticos de um primo ímpar  $p$ .

Aula 2: Critério de Euler. Se  $p$  é um primo ímpar então o número de resíduos quadráticos não nulos de  $p$  e o número de resíduos não quadráticos de  $p$  são iguais.

Aula 3: Símbolo de Legendre e suas propriedades. Determinação de  $(-1/p)$  para um primo ímpar  $p$ . Infinitude de primos da forma  $4k+1$ . Teorema de Lagrange: Todo polinômio não constante em  $\mathbb{Z}_p$  de grau  $n$  possui no máximo  $n$  raízes.

Aula 4: Lema de Gauss. Lema de Eisenstein. Lei de Reciprocidade Quadrática.

Aula 5: 08/07: feriado

Aula 6: Aplicações da Lei de Reciprocidade Quadrática. Símbolo de Jacobi. Propriedades.

Aula 7: Congruências quadráticas com módulo composto. Caracterização de quando a congruência  $x^2=a \pmod{n}$  é solúvel ( $\text{mdc}(a,n)=1$ ).

Aula 8: introdução ao estudo de formas quadráticas binárias com coeficientes inteiros. A topografia no plano bidimensional. Os movimentos de pular e saltar.

Interpretação de área dada pelo determinante. Teorema de Pick para paralelogramos. Vetor primitivo.

Aula 9: Vetores relaxados. Base relaxada. Domínio topográfico. Conexidade do topógrafo. Tríade.

Aula 10: Superbase estrita. Superbase relaxada. Orientação do topógrafo por determinantes.

Aula 11: Uniformidade da topografia.

Aula 12: Início ao estudo de equações diofantinas quadráticas utilizando a topografia para visualizar suas soluções. Formas binárias quadráticas. Alcance da topografia. Regra da progressão aritmética.

Aula 13: P1

Aula 14: Formas quadráticas definidas. Princípio de subida de Conway. Poços únicos e duplos. Existência e unicidade de poços.

Aula 15: Caminhos simples. Loops. Árvores. Caracterização de primos como soma de dois quadrados.

Aula 16: Se  $p$  é primo com  $p \equiv 1 \pmod{3}$  então a equação diofantina  $x^2 + xy + y^2 = p$  possui uma solução.

Aula 17: 19/08: feriado

Aula 18: Isometrias próprias de uma forma quadrática binária definida positiva.

Aula 19: Classificação de formas de discriminante zero.

Aula 20: Lagos e rios. Formas indefinidas.

Aula 21: O discriminante conta lagos. Unicidade dos rios. Periodicidade dos rios. Seja  $q(x,y)$  uma forma binária quadrática de discriminante que não é um quadrado, positivo. Seja  $N$  inteiro positivo, se a equação diofantina  $q(x,y) = N$  possui uma solução então ela possui infinitas soluções.

Aula 22: Infinitude de soluções da equação de Pell.

Aula 23: L

Aula 24: Revisão da matéria.

Aula 25: 16/09 - Prova Recuperação REC

Avaliação:

O desempenho dos discentes será avaliado através de provas dissertativas, listas de exercícios.

$M = (P1+L)/2$ , onde P1 nota da prova 1, L lista para entrega: será informada posteriormente.

P1: 05/08

L: 09/09

REC: 16/09

Caso o discente realize a prova de recuperação REC, a média final será calculada obrigatoriamente pela expressão  $M_{Final} = (M+REC)/2$ . Caso o discente não realize a prova de recuperação a média final será dada por  $M = (P1+L)/2$ .

Conceitos:

$8,5 \leq A \leq 10$

$7,0 \leq B < 8,5$

$5,0 \leq C < 7,0$

$4,5 \leq D < 5,0$

$0 \leq F < 4,5$

### **Lista de exercícios para a P1: [lista1](#)**

Bibliografia Básica:

BOREVICH, Z. I.; SHAFAREVICH, I. R. Number Theory. London: Academic Press, 1967.

IRELAND, K.; ROSEN, M. Classical Introduction to Modern Number Theory. New York: Springer-Verlag, 2010.

NIVEN, I.; ZUCKERMAN, H. S.; MONTGOMERY, H. L. An introduction to number theory. 5th ed. New York: John Wiley & Sons, 1991.

Bibliografia complementar:

COHN, H. Advanced number theory. Mineola. NY: Dover Publications, 1980.

DENCE, J. B.; DENCE, T. P. Elements of the Theory of Numbers. London: Academic Press, 1999.

HUA, L.-K. Introduction to number theory. Berlin-Heidelberg: Springer-Verlag, 1982.

LEVEQUE, W. J. Topics in Number Theory. Mineola. NY: Dover Publications, 2002.

ROSE, H.E. A Course in Number Theory. 2nd ed. Oxford: Oxford University Press, 1995.